REMARKS

This amendment is submitted in reply to the Office Action dated November 13, 2006. Claims 1-32 currently stand rejected. Applicant has amended independent claims 1, 8, 15, 22 and 25 and dependent claim 18 to more particularly distinguish the claimed invention from the cited references. Claims 7, 9, 13, 14, 17, 24 and 28 have been amended to correct typographical errors and for consistency of terminology. Applicants have also made amendment to the specification for purposes of clarity and consistency of terminology. For example, the specification has been amended to change references to first and second temporary secret keys to first and second temporary keys, respectively, to conform to the recitations provided for these respective elements in the claims. Similarly, Applicants have amended the term "predetermined secret key" to state instead "predefined secret key" for consistency, for example, with the recitation of claim 4. Finally, Applicants have amended certain portions of the specification to further define that the transforming of the first intermediate value and the predefined key change information may be performed by hashing. Independent claims 1, 12, 15, 22 and 25 have also been amended to incorporate this change. Support for these amendments can be found at least at page 7, lines 19-21 of the application as filed. No new matter has been added by the amendment. Claims 5 and 11 have been canceled, without prejudice.

In light of the amendment and the remarks presented below, Applicants respectfully request reconsideration and allowance of all now-pending claims of the present application.

Specification Objections

The specification stands objected to for including an informality in that page 11, lines 24-25 describes a "public key". Applicants note that the passage to which the Office Action objects was a typographical error, which has been corrected by the amendment to the specification. As indicated by the Examiner, support for the amendment is provided by the remainder of Applicants' disclosure which describes secret/symmetric key data encryption. Accordingly Applicants respectfully request that the objection to the specification be withdrawn.

Claim Objections

The Office Action objects to claim 20 for containing an informality in the form of a typographical error. Applicant has amended claim 20 to correct the informality. Accordingly Applicants respectfully request that the objection to claim 20 be withdrawn.

Claim Rejections - 35 USC §112

Claims 12-32 currently stand rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement. In this regard, the Office Action has pointed out a discrepancy in Applicants disclosure, which occurred due to a typographical error. Specifically, the description identified by the Office Action extending from lines 19 to 28 of page 17 of the application as filed included typographical errors. Applicant has amended the corresponding paragraph to correct the typographical errors. In this regard, amendments have been made to the disclosure extending from page 17, lines 19-28 to ensure agreement with the correct explanations provided at page 14, lines 17-25 and page 17, lines 8-12 with regard to modifying the secret key if the key change information has repeated and not modifying the second temporary key (i.e., the second temporary key is considered the final key value) if the key change information has not repeated.

Applicants also respectfully note that the criteria for indicating whether the key change information has repeated were also subject to a typographical error, which has been corrected by the present amendment. In this regard, as described at page 17, lines 12-19, the key change information serves as a counter that increments by one for each different secret key that is generated and then is reset once the key changing information repeats. Thus, repetition of the key change information is determined by checking the key change information to see if it equals 0xFF, thereby indicating that 256 secret keys have been generated without having the key change information repeat. Lines 19-28 of page 17 have been amended to correspond to this accurate description by indicating that a value of the key change information being equal to 0xFF indicates that the key change information has repeated and a value less than 0xFF indicates that the key change information has not repeated. Given the above described amendments to the specification, which have support based on the original disclosure of the Application as filed,

Applicants respectfully submit that there is no discrepancy in the description provided by specification and thus claim 12 is properly enabled.

Specifically, the Office Action has indicated that claim 12 recites "differently processing the first secret key to generate the key for data encryption in instances in which the key change information has repeated than in instances in which the key change information has not repeated". The amended specification now consistently describes modifying the first secret key in instances where the key change information has repeated and not modifying the first secret key in instances where the key change information has not repeated. Thus, there is clear support and enablement with regard to the claimed feature of "differently processing the first secret key to generate the key for data encryption in instances in which the key change information has repeated than in instances in which the key change information has not repeated" as recited in independent claim 12.

Applicants further note that independent claims 15, 22 and 25 do not include the same recitation as independent claim 12. To the contrary, independent claims 15, 22 and 25 recite generating a final key based upon the second temporary key and the determination if the predefined key change information has repeated, which feature is clearly described at page 14, lines 17-25, page 17, lines 8-12 and the amended passages at page 17, lines 19-28 of the present application. As such, Applicants respectfully submit that claims 15, 22 and 25 comply with the enablement requirement.

Claims 23, 24 and 26 currently stand rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement. Applicants respectfully traverse.

The Office Action states that there is not adequate information provided by the specification as to how the claimed system decrypts the data if the data is originally encrypted in accordance with the predetermined encryption technique, prior to encrypting the data transmitted via the communication network with the final key as provided in claims 23 and 26. However, Applicants respectfully submit that one of skill in the art could easily determine how to implement the claimed feature based only on the disclosure of claims 23 and 26, when read in light of the foundation provided by the remainder of the specification. Applicants have added the feature described in claims 23 and 26 to the specification based on the support originally

provided by the disclosure of claims 23 and 26. Accordingly, Applicants respectfully submit that the rejections of claims 23 and 26 as failing to comply with the enablement requirement are overcome. Claim 24 depends directly from claim 23 and appears to be rejected only on the basis of its dependency from claim 23. However, since the rejection of claim 23 on the basis of lack of enablement is overcome, so also is the rejection of claim 24, by virtue of the dependency of claim 24 from claim 23.

Claims 7, 9 and 14 currently stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. Specifically, the Office Action rejected claims 7, 9 and 14 based on specific recitations in each of claims 7, 9 and 14 for which there was not proper antecedent basis provided by the respective claims or the claims from which they depend. Applicants have amended claims 7, 9 and 14 to ensure proper antecedent basis is provided for each of the specific recitations identified in the Office Action. Accordingly, Applicants respectfully submit that the rejections of claims 7, 9 and 14 as being indefinite are overcome.

Claims 1-11 currently stand rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential steps. In this regard, the Office Action rejects claims 1-11 for being directed to only one phase of a three phase process for generating a key for data encryption. Independent claim 1 is directed to the first phase, while independent claim 8 is directed to the second phase. These claims are also rejected for reciting generation of a key for data encryption when, as the Office Action asserts, both claims only provide a temporary key.

In response to these rejections, Applicants initially note that there is no requirement that the Applicants must claim all three phases in the same claim. To the contrary, so long as each phase corresponds to a novel phase, Applicants believe they are entitled to claim each such novel phase separately. As such, Applicants respectfully submit that each of independent claim 1 and independent claim 8 corresponds to a novel phase for generating a temporary key, which when used in combination with each other and a third phase, result in a novel method for generating a final key. In order to clarify the relationship described above, Applicants have amended the preambles of both independent claims 1 and 8 to clarify that the corresponding independent claims are directed to a method for generating a temporary key.

In view of the fact that independent claims 1 and 8 are now clearly directed to methods for generating a temporary key, and in view of the further fact that such methods are each distinctly novel phases of a novel method, Applicants respectfully submit that the rejections of independent claims 1 and 8 and their corresponding dependent claims as being indefinite as being incomplete for omitting essential steps are overcome.

Claims 12-14 currently stand rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential steps. Applicants respectfully traverse.

The Office Action states that without certain additional features, the first secret key of independent claim 8 would be the same as a WEP key. As such, the Office Action apparently assumes that the output of independent claim 8 is necessarily the input of independent claim 12 since independent claim 12 recites "calculating a first secret key utilizing predefined key change information" and independent claim 8 refers to a first secret key. However, Applicants respectfully note that independent claim 12 does not depend from independent claim 8. As such, it would appear that the importation of judgments made with respect to the subject matter of independent claim 8, are not appropriate when evaluating the patentability of independent claim 12. Moreover, independent claim 12 is directed to a method which does not omit any essential steps. Whether or not the first secret key calculated in independent claim 12 is calculated according to the method disclosed in another claim, or whether the first secret key is the same or different from a WEP key is immaterial to the fact that the calculated first secret key is processed differently based on a determination with regard to whether or not the key change information has repeated as provided in independent claim 12. Accordingly, independent claim 12, when read properly as an independent claim, does not omit any essential steps. Therefore, Applicants respectfully submit that the rejections of claims 12-14 as being incomplete are overcome.

For all the reasons above, Applicants respectfully submit that the rejections of claims 1-32 under 35 U.S.C. §112, first and second paragraphs are overcome.

Claim Rejections

Claims 1-8, 11, 12, 14-16, 18-20, 22, 25, 27 and 29-32 currently stand rejected under 35 U.S.C. §102(a), as being anticipated by Housley et al. ("Alternate Temporal Key Hash",

hereinafter "Housley"). Claim 8 also stands rejected under 35 U.S.C. §102(b), as being anticipated by "ANSI/IEEE Std 802.11 – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" (hereinafter "802.11 Standard"). Claims 9, 10 and 21 stand rejected as being unpatentable over the 802.11 Standard in view of Housley. Claims 13, 17 and 28 stand rejected as being unpatentable over Housley in view of Kelem et al. (U.S. Patent No. 6,118,869, hereinafter "Kelem"). As stated above, claims 5 and 11 have been canceled, without prejudice, thus the rejections of claims 5 and 11 are now moot.

Independent claim 1 has been amended to recite, *inter alia*, combining the first secret key with at least a portion of a user-specific Medium Access Control (MAC) address by performing a bitwise exclusive OR (XOR) operation to result in an intermediate value.

Housley is directed to a method for processing a temporal key to derive a per-packet key. Section 3 of Housley describes an alternate temporal key hash function in which a P1K, which the Office Action apparently interprets as an intermediate value, is calculated based on a temporal key (TK) and at transmitter address (TA). The P1K is then combined with IV16, which the Office Action apparently interprets as predefined key change information, to generate a key for encryption.

Sections 3, 5 and 6 of Housley also disclose the use of a XOR function with respect to certain values within the generated key. However, Applicants respectfully note that with respect to the rejection of independent claim 1, although Housley discloses an XOR operation, the XOR operation of Housley is not performed with respect to the first secret key and at least a portion of the MAC address as indicated, for example, by the description of Phase 2 at page 3 of Housley. In fact, Housley fails to teach or suggest any XOR operation including a user specific MAC address as provided in independent claim 1. Independent claim 1 has also been amended to recite transforming the combination of the intermediate value with the predefined key change information by hashing, which Applicants respectfully submit is also neither taught nor suggested in Housley. Thus, the subject matter of independent claim 1 is neither anticipated nor obvious in view of Housley. Although not cited in connection with the rejection of independent claim 1, the 802.11 Standard and Kelem fail to cure the deficiencies of Housley described above.

Independent claim 8 has been amended to recite, *inter alia*, permutating the intermediate value by exchanging a selected number of bits of the IV value with an equal number of other bits of the IV value and outputting a result of a bitwise XOR operation and the exchange of the bits as a value that is bit shifted. With respect to the rejections of independent claim 8, we would note that it is unclear as to which portion of section 3 of Housley is being interpreted to correspond to the recited permutation feature of independent claim 8. However, regardless of which feature is being read to correspond to the permutation feature of independent claim 8, there is no disclosure in Housley that defines any permutation feature as exchanging bits of the IV value and outputting a result of the bitwise XOR operation and exchange of the bits as a value that is bit shifted as provided in independent claim 8 and as defined at page 16, lines 19-27 of the specification. Applicants also note that the 802.11 Standard similarly fails to provide any teaching or suggestion of permutation as currently defined in independent claim 8. Accordingly, the subject matter of independent claim 8 is neither anticipated nor obvious in view of Housley or the 802.11 Standard either alone or in combination. Although not cited in connection with the rejection of independent claim 8, Kelem fails to cure the deficiencies of Housley described above.

Claims 12, 15, 22 and 25 each refer to a determination of whether predefined key change information has repeated. Claim 12 also refers to different processing for the first secret key to generate the key for data encryption in instances where the key change information has repeated than in instances in which the key change information has not repeated. The Office Action cites Housley as disclosing such feature at section 5 of Housley, but provides no specific indication of which portion of section 5 meets the claimed feature. Upon reviewing all of section 5, Applicants could find no disclosure in the cited passage or all of Housley regarding determining whether key change information has repeated or different processing for the first secret key to generate the key for data encryption in instances where the key change information has repeated than in instances in which the key change information has not repeated as provided in independent claim 12. Although Housley discusses a concern over reuse of the same key, Housley discloses methods to decrease the likelihood of such reuse and fails to teach or suggest both determining whether predefined key change information has repeated and differently

processing the first secret key to generate the key for data encryption in instances where the key change information has repeated than in instances in which the key change information has not repeated as recited in independent claim 12. The 802.11 Standard and Kelem also fail to teach or suggest the above recited feature of independent claim 12 and are not cited as such. Thus, the cited references, either individually or in combination, fail to teach or suggest the recited features of independent claim 12.

As stated above, independent claims 15, 22 and 25 also recite determining if predefined key change information has repeated, which is not taught or suggested in any of the cited references either individually or in combination. Claims 15, 22 and 25 also refer to generation of a final key based on the second temporary key and the determination that the key change information has repeated if the predetermined key change information has repeated. This feature is also neither taught nor suggested in any of the cited references either individually or in combination. Accordingly, independent claims 15, 22 and 25 are patentable over the cited references taken either individually or in combination.

Dependent claims 2-4, 6, 7, 9, 10, 13, 14, 16-21, 23, 24 and 26-32 depend either directly or indirectly from respective ones of independent claims 1, 8, 12, 15, 22 and 25 and thus include all the recitations of their respective independent claims. Therefore, dependent claims 2-4, 6, 7, 9, 10, 13, 14, 16-21, 23, 24 and 26-32 are patentable for at least those reasons given above for independent claims 1, 8, 12, 15, 22 and 25.

Accordingly, Applicants respectfully submit that the rejections of claims 1-4, 6-10 and 12-32 are overcome.

CONCLUSION

In view of the amendment and remarks submitted above, it is respectfully submitted that the present claims are in condition for immediate allowance. It is therefore respectfully requested that a Notice of Allowance be issued. The Examiner is encouraged to contact Applicants' undersigned attorney to resolve any remaining issues in order to expedite examination of the present invention.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.

Respectfully submitted,

Chad L. Thorson
Registration No. 55,675

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

ELECTRONICALLY FILED USING THE EFS-WEB ELECTRONIC FILING SYSTEM OF THE UNITED STATES PATENT & TRADEMARK OFFICE ON FEBRUARY 13, 2007.